Input Validation

Paul Mooney
Chief Software Architect, Microsoft MVP

@daishisystems | www.insidethecpu.com

Overview

Input Validation in a Nutshell

- Prevent attacks like SQL Injection
- Built-in validation functions
- Remove malicious content
- Whitelisting
- Boundary-checking
- Character-escaping

Demo

Techniques to Ensure Data Validity

- Set up our development environment
- Install Go
- Install Postman

Ensuring Data Validity: Whitelisting

Defining a list of allowed values or patterns

Boundary Checking

Ensuring that user input is within a defined range

Character Escaping

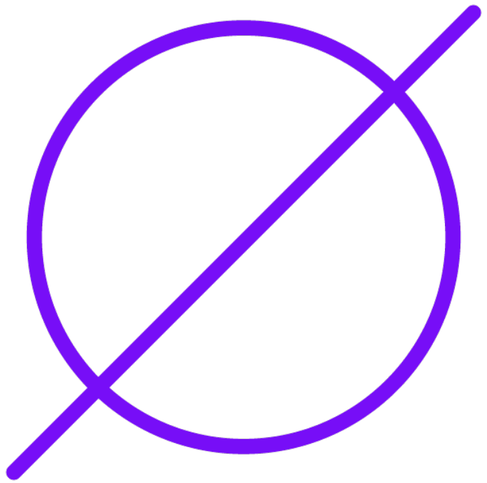
Preventing attacks such as cross-site scripting

Numeric Validation

Ensuring that numeric inputs are safe and dependable

Checking for Null Bytes

Preventing unexpected issues with strings

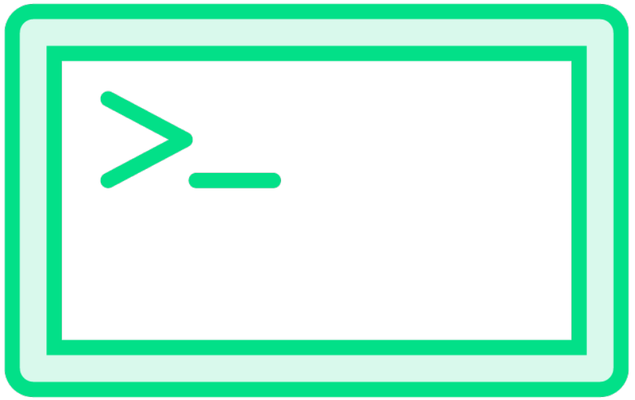


What is a Null byte?

- Null terminator
- Null character
- Character string end
- \x00
- Indicate string end prematurely
- Unexpected behavior

Checking for New Line Characters

Preventing unexpected issues with strings

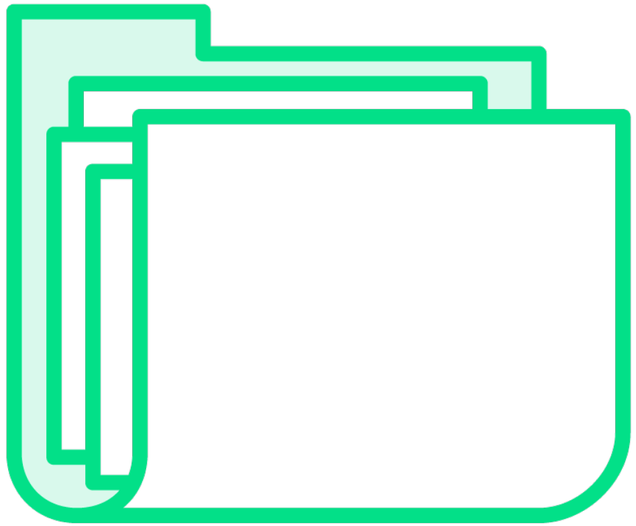


What is a Newline character?

- End of a line of text
- Byte value 10
- Inject malicious code

Identifying Path Alteration Characters

Protecting files and directories from unauthorized access

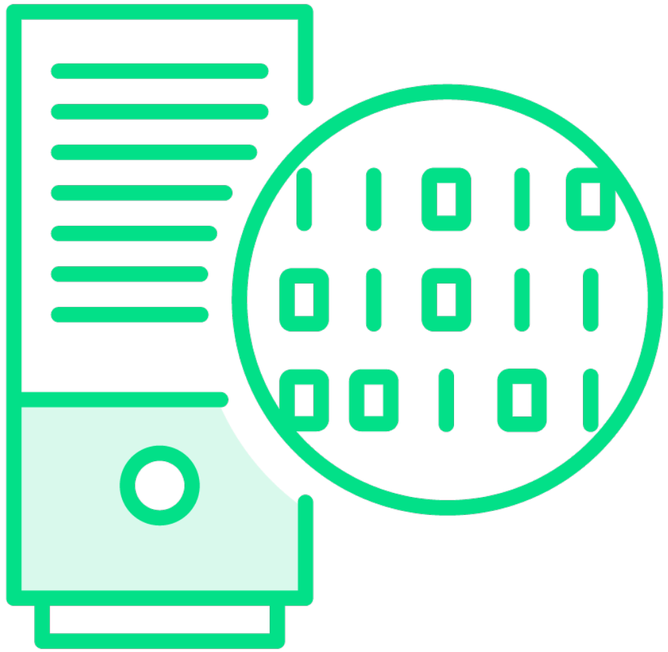


What is a path-alteration character?

- Directory traversal character
- Navigate between filesystems
- Access files and directories

Validating Extended UTF-8 Encoding

Preventing input validation-bypass attacks



What is Extended UTF-8 Encoding?

- Variation of UTF-8 encoding scheme
- Encoding beyond standard Unicode range
- Can bypass input validation

Summary

Input Validation

- Whitelisting
- Boundary-checking
- Character-escaping
- Erroneous user input
- Threat actors
- Input validation is only the first step